7. ABSTRACT

The subject of the disclosed technology is shown in the following. In the information processing device such as an IC card the overflow processing which occurs in the case of a modular multiplication operation to be performed during crypto-processing inside shows a particular pattern of a consumption current. It is the subject of the present invention to decrease the relationship between data processing and the pattern of the consumption current.

Means for improving the problem is shown in the following. In the processing procedures for performing a modular exponentiation operation according to the 2 bit addition chain method, modular multiplication operation to be executed is selected at random in step 1106, the selected modular multiplication operation is executed for each 2 bits in a step among step 1112 to step 1115, the correction of the result is performed in step 1116, and in step 1118 or 1119, the result of the calculation (corrected value or uncorrected value) is output.